IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	)	
	)	
Agostinho DeArruda Villela	)	Group Art Unit: 2131
	)	
Serial No. 10/598,719	)	Examiner: Wright, Bryan F
	)	
Filed: September 8, 2006	)	
	)	
For: Access Control System For Information Services Based On Hardware And Software Signature Of A Requesting Device	)	

APPEAL BRIEF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	)	
	)	
Agostinho DeArruda Villela	)	Group Art Unit: 2131
	)	
Serial No. 10/598,719	)	Examiner: Wright, Bryan F
	)	
Filed: September 8, 2006	)	
	)	
For: Access Control System For Information Services Based On Hardware And Software Signature Of A Requesting Device	)	

APPEAL BRIEF

I. INTRODUCTION

This is an appeal from the decision mailed October 15, 2009 of the Patent Examiner, Group Art Unit 2131, finally rejecting claims 17-30 and 35 under 35 U.S.C. §103 as being obvious by Chaung in view of Matsuzaki and further in view of Drew, and rejecting claims 31-34 under 35 U.S.C. §103 as being obvious by IE020429 in view of Matsuzaki and further in view of Drew.

II. REAL PARTY IN INTEREST

The Applicant is the real party in interest.

III. RELATED APPEALS AND INTERFERENCES

None.

IV. STATUS OF THE CLAIMS

Claims 17-35 stand rejected by the action mailed October 15, 2009. Claims 17-35 are pending. Applicant hereby appeals the rejection of claims 17-35.

V. STATUS OF AMENDMENTS

None.

VI. SUMMARY OF CLAIMED SUBJECT MATTER

Applicant's claim 17 claims a method for identifying devices and controlling access to a service (page 5, lines 1-7), comprising the steps of collecting data related to software and hardware configurations from a device through a software agent (page 5, lines 8-14), generating a digital signature (page 5, lines 15-20) for the device by hashing the software and hardware configuration data (page 8, lines 1-8), sending the digital signature of the device to an authentication server (page 5, lines 21-24), and determining whether the device has been excluded from accessing or enrolling in the service (page 9, lines 6-10).

Applicant's claim 31 claims a method for identifying devices and controlling access to a service (page 5, lines 1-7) comprising the steps of collecting data related to software and hardware configurations from the device through a software agent (page 5, lines 8-14), generating a digital signature (page 5, lines 15-20) for the device by hashing the software and hardware configuration data (page 8, lines 1-8), sending the digital signature of the device to the authentication server (page 5, lines 21-24), verifying that the device is not on a list or in a group of devices not allowed to access the service (page 9, lines 6-10), or is not a device with a maximum number of enrollments set to zero (page 9,

lines 6-10), and registering the device as authorized to access the service (page 7, lines 10-24).

Applicant's claim 35 claims a system for identifying devices and controlling access to a service (page 5, lines 1-7) comprising a software agent installed on a device (page 5, lines 8-14) adapted to collect data related to software and hardware configuration of the device (page 5, liens 8-14), a digital signature for the device generated by the software agent by hashing the software and hardware configuration data (page 8, lines 1-8), and an authentication server that determines whether the device can access the service based upon the digital signature of the device (page 5, lines 21-24), wherein the authentication server verifies that the device is not a list or in a group of devices not allowed to access the service (page 9, lines 6-10), or is not a device with a maximum number of enrollments set to zero (page 9, lines 6-10).

VII. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 17-30 and 35 stand rejected under 35 U.S.C. §103 as being obvious by Chaung in view of Matsuzaki and further in view of Drew. Claims 31-34 stand rejected under 35 U.S.C. §103 as being obvious by IE020429 in view of Matsuzaki and further in view of Drew.

VIII. ARGUMENT

(A) Claim 17 rejected under Section 103

The examiner has rejected claim 17 under 35 U.S.C. §103 as being made obvious by Chaung in view of Matsuzaki and further in view of Drew.

Applicant's claim 17 specifically describes the method as including the step of "collecting data related to software and hardware configurations from a device through a software agent". The examiner contends that the Chaung patent shows this feature, the examiner even pointing to paragraph 38 of the Chaung reference. However, upon examination of the Chaung patent it is clear that this references shows the gathering of software data, but does not show the gathering of hardware data. It should be noted that "files" are considered software data and not hardware. The Chaung reference specifically states in Paragraph 0033 that the

"system is first set up by calculating and archiving fingerprints for all files relating to operating system or application software".

The Chaung references further describes how the system verifies the client through "servers address", again illustrating the fact that the verification is predicated upon software and not hardware data (see paragraph 0037).

Applicant respectfully points out that the paragraph specifically pointed out by the examiner (paragraph 0038) actually contradicts the examiner's position and supports the Applicant's position. In this paragraph it is recited that

"On the server 14, each hash result for each file on the client system is compared against what are the expected hash values given certain parameters such as the client system's operating system version and software patch/update level. This expected hash information is fetched from the database of acceptable file fingerprints 16 which houses all the pre-calculated hash values for all files in various operating systems and application."

Again, this illustrates that the verification is based upon software parameters rather than hardware parameters or a combination of each.

Applicant submits that it is this hardware data verification that distinguishes the present application from the prior art. Software may be reproduced, cloned or modified, however, it is much more difficult to change or copy hardware data. The inclusion of this hardware data significantly increases the protection of the transmission. This hardware data verification has not been shown in the Chaung patent and thus does not render claim 17 obvious as suggested by the examiner.

Applicant's Claim 17 also includes the step of "determining whether the device has been excluded from accessing or enrolling in the service. Contrary to the examiner's statement, the Matsuzaki patent does not disclose determining whether the device has been excluded from accessing or enrolling in the service. Matsuzaki discloses a system for the registration of multiple devices within a particular group, and describes limiting the number of devices enrolled, but not whether the device has been excluded from accessing or enrolling in the service. In Matsuzaki, registration fails if the total number of devices enrolled exceeds a set figure, not if the particular device has been excluded from accessing or enrolling in the service.

The Examiner has cited the combination of three separate references to describe the entire method of claim 17 and then asserts that a person of ordinary skill in the art would have recognized the desirability and advantage of modifying Chaung by employing the features disclosed in Matsuzaki and Drew, for which digital signature generation will be enhanced.

However, the Examiner has failed to make a prima facie case of obviousness under Section 103. The rejection contains no statement that supports a motivation to combine these three pieces of prior

art to develop the Applicant's claimed invention, other that the conclusory assertion that one of ordinary skill in the art would have recognized the desirability and advantage of the combination. Conclusory statements of generalized advantages are inadequate to support a finding of motivation. *See. e.g., In re Beasley,* 2004 WL 2793170 (Fed. Cir. Dec. 7, 2004) (slip op. at 10). The examiner must present a "convincing line of reasoning" as to why the combination of teachings is proper. MPEP 2142. There is no such line of reasoning in the rejection, and a prima facie case has not been made.

It is well settled that the obviousness of an invention cannot be established by combining the teaching of the prior art absent some teaching, suggestion or incentive supporting the combination, see *In re Fine,* 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *Ashland Oil, Inc. v. Delta Resins and Refractories, Inc.,* 776 F.2d 281, 227 USPQ 657 (Fed. Cir. 1985) ; *ACS Hospital Systems, Inc. v. Montefiore Hospital,* 732 F,2d 1572, 221 USPQ 929 (Fed. Cir. 1984) *Pentec, Inc. v Graphic Controls Corp.,* 776 F.2d 309, 227 USPQ 766 (Fed,Cir. 1985). Moreover, the mere fact that the prior art could be modified in the manner suggested by the examiner does not make such a modification obvious unless the prior art fairly suggests the desirability of the modification, see *In re Gordon,* 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984) . Here, the references do not suggest any motivation for, or the desirability of, Applicant's unique method of utilizing hardware data to verify access and to exclude devices from accessing the service. As such, it is improper to utilize these references to establish obviousness.

It is acknowledged that the tendency to resort to "hindsight" based upon applicant's disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion

must be reached on the basis of the facts gleaned from the prior art. MPEP 2142. This is "especially important in the case of less technologically complex inventions, where the very ease with which the invention can be understood may prompt one 'to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher.'". *In re Dembiczak*, 175 F.3d 994, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999) citing *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1553, 220 USPQ 303, 313 (Fed. Cir. 1983) . With this in mind, a hindsight-based obviousness analysis must be supported by evidence which is "clear and particular". *In re Dembiczak*. It is insufficient to simply offer a broad range of sources or to make conclusory statements, as "[broad conclusory statements regarding the teaching of multiple references, standing along, are not 'evidence'". *Id*. Applicant respectfully submits that the examiner has claimed the present invention to be obvious utilizing hindsight, speculation and conclusory statements which are not, in fact, supported by the cited references, to come up with a combination that would either destroy the clear intention of the reference or modify such in a manner that goes against the clear teachings of the reference. Furthermore, it is submitted that it is only through such hindsight that the Applicant's invention of an access control system and method can be gleamed from the cited references. Applicant respectfully contends that the invention is not obvious or a designer's choice, but instead is novel and therefore worthy of patent protection.

Applicant respectfully submits that the invention described in Claim 17 is novel and worthy of patent protection.

(B) Claim 31 under Section 103

The examiner has rejected claim 31 under 35 U.S.C. §103 as being made obvious by IE020429 in view of Matsuzaki and further in view of Drew.

Applicant's claim 31 specifically describes the method as including the step of "collecting data related to software and hardware configurations from a device through a software agent". The examiner contends that the IE020429 patent shows this feature, the examiner even pointing to page 14 of the IE020429 reference. However, upon examination of the IE020429 patent it is clear that this references shows the gathering of software data, but does not show the gathering of hardware data. The IE020429 reference specifically states in Page 14 that the system utilizes timing sequences to create a fingerprint. These timing sequences are based upon the time it takes a specific system to complete a given task (see pages 3-6), based on latency, tolerable imperfections I the components, the assembly of the system and other random variables governing the response time for a set of measurements.. The use of this timing sequence is not all the same as the collecting of data related to software and hardware configurations from the device.

The IE020429 patent specifically states on Page 11, which was cited by the examiner, that "[A]nalysis of statistical parameters of logged series of measurements revealed that it is possible to employ these time measurements to discriminate between such nearly identical systems, and that it is this timing that is utilized to verify the system. Specifically,

"[I]n a personal computer, various other possibilities exist for development of time series for access to devices on the PCI bus (network cards, graphic cards, etc.) and IDE devices (hard drives, disk drives, CD-ROMS, etc.). Information obtained for these

devices provide more variety and possibilities for obtaining a fingerprint of the system."

This verification or fingerprint is all based on time calculations not hardware data configurations.

Applicant submits that it is this hardware data verification that distinguishes the present application from the prior art. Software may be reproduced, cloned or modified, however, it is much more difficult to change or copy hardware data. The inclusion of this hardware data significantly increases the protection of the transmission. This hardware data verification has not been shown in the IE020429 patent and thus does not render claim 31 obvious as suggested by the examiner.

Applicant's Claim 31 also includes the step of "determining whether the device has been excluded from accessing or enrolling in the service. Contrary to the examiner's statement, the Matsuzaki patent does not disclose determining whether the device has been excluded from accessing or enrolling in the service. Matsuzaki discloses a system for the registration of multiple devices within a particular group, and describes limiting the number of devices enrolled, but not whether the device has been excluded from accessing or enrolling in the service. In Matsuzaki, registration fails if the total number of devices enrolled exceeds a set figure, not if the particular device has been excluded from accessing or enrolling in the service.

The Examiner has cited the combination of three separate references to describe the entire method of claim 31 and then asserts that a person of ordinary skill in the art would have recognized the desirability and advantage of modifying IE020429 by employing the features disclosed in Matsuzaki and Drew, for which digital signature generation will be enhanced.

However, the Examiner has failed to make a prima facie case of

obviousness under Section 103. The rejection contains no statement that supports a motivation to combine these three pieces of prior art to develop the Applicant's claimed invention, other that the conclusory assertion that one of ordinary skill in the art would have recognized the desirability and advantage of the combination. Conclusory statements of generalized advantages are inadequate to support a finding of motivation. *See. e.g., In re Beasley,* 2004 WL 2793170 (Fed. Cir. Dec. 7, 2004) (slip op. at 10). The examiner must present a "convincing line of reasoning" as to why the combination of teachings is proper. MPEP 2142. There is no such line of reasoning in the rejection, and a prima facie case has not been made.

It is well settled that the obviousness of an invention cannot be established by combining the teaching of the prior art absent some teaching, suggestion or incentive supporting the combination, see *In re Fine,* 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *Ashland Oil, Inc. v. Delta Resins and Refractories, Inc.,* 776 F.2d 281, 227 USPQ 657 (Fed. Cir. 1985) ; *ACS Hospital Systems, Inc. v. Montefiore Hospital,* 732 F,2d 1572, 221 USPQ 929 (Fed. Cir. 1984) *Pentec, Inc. v Graphic Controls Corp.,* 776 F.2d 309, 227 USPQ 766 (Fed,Cir. 1985). Moreover, the mere fact that the prior art could be modified in the manner suggested by the examiner does not make such a modification obvious unless the prior art fairly suggests the desirability of the modification, see *In re Gordon,* 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984) . Here, the references do not suggest any motivation for, or the desirability of, Applicant's unique method of utilizing hardware data to verify access and to exclude devices from accessing the service. As such, it is improper to utilize these references to establish obviousness.

It is acknowledged that the tendency to resort to "hindsight" based upon applicant's disclosure is often difficult to avoid due

to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art. MPEP 2142. This is "especially important in the case of less technologically complex inventions, where the very ease with which the invention can be understood may prompt one 'to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher.'". *In re Dembiczak*, 175 F.3d 994, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999) citing *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1553, 220 USPQ 303, 313 (Fed. Cir. 1983) . With this in mind, a hindsight-based obviousness analysis must be supported by evidence which is "clear and particular". *In re Dembiczak*. It is insufficient to simply offer a broad range of sources or to make conclusory statements, as "[broad conclusory statements regarding the teaching of multiple references, standing along, are not 'evidence'". *Id.* Applicant respectfully submits that the examiner has claimed the present invention to be obvious utilizing hindsight, speculation and conclusory statements which are not, in fact, supported by the cited references, to come up with a combination that would either destroy the clear intention of the reference or modify such in a manner that goes against the clear teachings of the reference. Furthermore, it is submitted that it is only through such hindsight that the Applicant's invention of an access control system and method can be gleamed from the cited references. Applicant respectfully contends that the invention is not obvious or a designer's choice, but instead is novel and therefore worthy of patent protection.

Applicant respectfully submits that the invention described in Claim 31 is novel and worthy of patent protection.

(B) Claim 35 under Section 103

The examiner has rejected claim 35 under 35 U.S.C. §103 as being made obvious by Chaung in view of Matsuzaki and further in view of Drew.

Applicant's claim 35 specifically describes the method as including the step of having "a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device" and "hashing the software and hardware configuration data". The examiner contends that the Chaung patent shows this feature, the examiner even pointing to paragraph 38 of the Chaung reference. However, upon examination of the Chaung patent it is clear that this references shows the gathering and hashing of software data, but does not show the gathering and hashing of hardware data. It should be noted that "files" are considered software data and not hardware. The Chaung reference specifically states in Paragraph 0033 that the

"system is first set up by calculating and archiving fingerprints for all files relating to operating system or application software".

The Chaung references further describes how the system verifies the client through "servers address", again illustrating the fact that the verification is predicated upon software and not hardware data (see paragraph 0037).

Applicant respectfully points out that the paragraph specifically pointed out by the examiner (paragraph 0038) actually contradicts the examiner's position and supports the Applicant's position. In this paragraph it is recited that

"On the server 14, each hash result for each file on the

client system is compared against what are the expected hash values given certain parameters such as the client system's operating system version and software patch/update level. This expected hash information is fetched from the database of acceptable file fingerprints 16 which houses all the pre-calculated hash values for all files in various operating systems and application."

Again, this illustrates that the verification is based upon software parameters rather than hardware parameters or a combination of each.

Applicant submits that it is this hardware data verification that distinguishes the present application from the prior art. Software may be reproduced, cloned or modified, however, it is much more difficult to change or copy hardware data. The inclusion of this hardware data significantly increases the protection of the transmission. This hardware data verification has not been shown in the Chaung patent and thus does not render claim 35 obvious as suggested by the examiner.

Applicant's Claim 35 also includes the step of verifying "that the device is not a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero". Contrary to the examiner's statement, the Matsuzaki patent does not disclose determining whether the device has been excluded from accessing or enrolling in the service. Matsuzaki discloses a system for the registration of multiple devices within a particular group, and describes limiting the number of devices enrolled, but not whether the device has been excluded from accessing or enrolling in the service. In Matsuzaki, registration fails if the total number of devices enrolled exceeds a set figure, not if the particular device has been excluded from accessing or enrolling in the service.

The Examiner has cited the combination of three separate

references to describe the entire method of claim 35 and then asserts that a person of ordinary skill in the art would have recognized the desirability and advantage of modifying Chaung by employing the features disclosed in Matsuzaki and Drew, for which digital signature generation will be enhanced.

However, the Examiner has failed to make a prima facie case of obviousness under Section 103. The rejection contains no statement that supports a motivation to combine these three pieces of prior art to develop the Applicant's claimed invention, other that the conclusory assertion that one of ordinary skill in the art would have recognized the desirability and advantage of the combination. Conclusory statements of generalized advantages are inadequate to support a finding of motivation. *See. e.g., In re Beasley*, 2004 WL 2793170 (Fed. Cir. Dec. 7, 2004) (slip op. at 10). The examiner must present a "convincing line of reasoning" as to why the combination of teachings is proper. MPEP 2142. There is no such line of reasoning in the rejection, and a prima facie case has not been made.

It is well settled that the obviousness of an invention cannot be established by combining the teaching of the prior art absent some teaching, suggestion or incentive supporting the combination, see *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *Ashland Oil, Inc. v. Delta Resins and Refractories, Inc.*, 776 F.2d 281, 227 USPQ 657 (Fed. Cir. 1985); *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F,2d 1572, 221 USPQ 929 (Fed. Cir. 1984) *Pentec, Inc. v Graphic Controls Corp.*, 776 F.2d 309, 227 USPQ 766 (Fed,Cir. 1985). Moreover, the mere fact that the prior art could be modified in the manner suggested by the examiner does not make such a modification obvious unless the prior art fairly suggests the desirability of the modification, see *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984) . Here, the references do not suggest any motivation for, or the desirability

of, Applicant's unique method of utilizing hardware data to verify access and to exclude devices from accessing the service. As such, it is improper to utilize these references to establish obviousness.

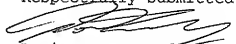
It is acknowledged that the tendency to resort to "hindsight" based upon applicant's disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art. MPEP 2142. This is "especially important in the case of less technologically complex inventions, where the very ease with which the invention can be understood may prompt one 'to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher.'". *In re Dembiczak*, 175 F.3d 994, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999) citing *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1553, 220 USPQ 303, 313 (Fed. Cir. 1983). With this in mind, a hindsight-based obviousness analysis must be supported by evidence which is "clear and particular". *In re Dembiczak*. It is insufficient to simply offer a broad range of sources or to make conclusory statements, as "[broad conclusory statements regarding the teaching of multiple references, standing along, are not 'evidence'". *Id.* Applicant respectfully submits that the examiner has claimed the present invention to be obvious utilizing hindsight, speculation and conclusory statements which are not, in fact, supported by the cited references, to come up with a combination that would either destroy the clear intention of the reference or modify such in a manner that goes against the clear teachings of the reference. Furthermore, it is submitted that it is only through such hindsight that the Applicant's invention of an access control system and method can be gleamed from the cited references. Applicant respectfully contends that the invention is

not obvious or a designer's choice, but instead is novel and therefore worthy of patent protection.

Applicant respectfully submits that the invention described in Claim 35 is novel and worthy of patent protection.

The requisite fee due upon filing of this brief was previously attached. Any additional fee is to be charged to Baker Donelson Bearman Caldwell & Berkowitz, PC, Deposit Account No. 11-0553.

Respectfully submitted,



Dorian B. Kennedy
Registration No. 38,840

BAKER DONELSON BEARMAN CALDWELL & BERKOWITZ
Suite 1600
3414 Peachtree Road NE
Atlanta, Georgia 30328
(678) 406-8705

Docket No.: 2171323-000002

CLAIMS APPENDIX

Claims 1-16 (canceled).

Claim 17. A method for identifying devices and controlling access to a service, comprising the steps of:

collecting data related to software and hardware configurations from a device through a software agent;

generating a digital signature for the device by hashing the software and hardware configuration data;

sending the digital signature of the device to an authentication server; and

determining whether the device has been excluded from accessing or enrolling in the service.

Claim 18. The method of claim 17, wherein the digital signature sent to the authentication server is encrypted.

Claim 19. The method of claim 17, wherein the software agent is installed on the device as part of the process of using the device to access a service.

Claim 20. The method of claim 17, wherein the hashes used to generate the digital signature are changed with every attempt to access a service, and the hashes cannot be reversed.

Claim 21. The method of claim 17, wherein the digital signature is one of several stages of a framework of authorization and authentication processes governing access to the service by the device.

Claim 22. The method of claim 17, wherein the authentication server compares the digital signature sent with one or more previously-stored digital signatures.

Claim 23. The method of claim 17, wherein the authentication server determines whether the device has been excluded from accessing or enrolling in the service by determining whether the device is on a list or in a group of devices not allowed to access the service, or is included within a group of devices allowed to access the service.

Claim 24. The method of claim 17, wherein the authentication server allows a maximum number of enrollments for a particular device.

Claim 25. The method of claim 24, wherein the maximum number of enrollments is zero.

Claim 26. The method of claim 22, wherein the authentication server allows minor modifications to the software or hardware configurations of a previously-enrolled device so as to preserve access or denial of access for the device.

Claim 27. The method of claim 26, wherein the previously-stored digital signature of the device is updated to reflect the modifications.

Claim 28. The method of claim 17, wherein the authentication server logs all accesses or attempted accesses by a device to the service.

Claim 29. The method of claim 17, wherein multiple devices can be registered for a single user with the authentication server to create a registration hierarchy.

Claim 30. The method of claim 29, wherein a user can unregister a device only through the device itself, or another device within the registration hierarchy registered earlier than the device to be unregistered.

Claim 31. A method for identifying devices and controlling access to a service, comprising the steps of:

collecting data related to software and hardware configurations from the device through a software agent;

generating a digital signature for the device by hashing the software and hardware configuration data;

sending the digital signature of the device to the authentication server;

verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero;

and registering the device as authorized to access the service.

Claim 32. The method of claim 31, further comprising the step of verifying the identity of the device each time it subsequently attempts to access the service.

Claim 33. The method of claim 32, wherein the step of verifying the identity of the device comprises the steps of:

collecting data related to current software and hardware configurations from the device through a software agent;

generating a digital signature for the device by hashing the

software and hardware configuration data;

sending the digital signature of the device to the authentication server; and

comparing the digital signature sent with one or more previously-stored digital signatures for the device.

Claim 34. The method of claim 32, wherein the step of verifying the identity of the device comprises the steps of:

collecting data related to current software and hardware configurations from the device through a software agent;

generating a digital signature for the device by hashing the software and hardware configuration data;

sending the digital signature of the device to the authentication server; and

verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero.

Claim 35. A system for identifying devices and controlling access to a service, comprising:

a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device;

a digital signature for the device, generated by the software agent by hashing the software and hardware configuration data; and

an authentication server that determines whether the device can access the service based upon the digital signature of the device;

wherein the authentication server verifies that the device is not a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None